

Patent

UNITED STATES PATENT APPLICATION

for

INTELLIGENT GATE-DISTRIBUTED USE
AND DEVICE NETWORK ACCESS MANAGEMENT
ON PERSONAL AREA NETWORK

Inventors:

ALAN RUBINSTEIN
GARY WANG

prepared by:

WAGNER, MURABITO & HAO, LLP
Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060

3COM-3721.BCG.US/JPW/MRH

INTELLIGENT GATE DISTRIBUTED USE
AND DEVICE NETWORK ACCESS MANAGEMENT
ON PERSONAL AREA NETWORK

RELATED U.S. APPLICATIONS

5 This application claims priority to the commonly-owned co-
pending provisional patent applications: patent application U.S.
serial number 60/277,593, entitled "INTELLIJACK' PHYSICAL
CONCEPTS," filed March 20, 2001, and assigned to the assignee of
the present invention; patent application U.S. serial number
10 60/277,767, entitled "A METHOD FOR MANAGING INTELLIGENT
HARDWARE FOR ACCESS TO VOICE AND DATA NETWORKS," filed March
20, 2001, and assigned to the assignee of the present invention;
patent application U.S. serial number 60/277,451, entitled "A
METHOD FOR FILTERING ACCESS TO VOICE AND DATA NETWORKS BY
15 USE OF INTELLIGENT HARDWARE," filed March 20, 2001, and assigned
to the assignee of the present invention; patent application U.S.
serial number 60/277,592, "INTELLIJACK' USAGE," filed March 20,
2001, and assigned to the assignee of the present invention; and
patent application U.S. serial number 60/285,419, "INTELLIGENT
20 CONCENTRATOR," filed April 20, 2001, and assigned to the assignee
of the present invention.

FIELD OF THE INVENTION

The present invention relates to the field of Personal Area Networking (PAN) and access to those networks by various wireless access devices. More specifically, the present invention relates to a
 5 device and system for intelligently managing access to wireless networks.

BACKGROUND OF THE INVENTION

Personal Area Networks are developing as adjuncts to local area networks (LANs). Modern personal area networking (PAN)
 10 generally refers to a small group of devices that communicate wirelessly and are normally within a small, personal, area. The PAN usually communicates with a network hub or a server that provides connection to a larger local area network (LAN) and to the Internet. Communication within the PAN is generally by RF or infrared devices
 15 and interface with the LAN is usually accomplished by cable connections between the wireless hub and the network server.

The wireless nature of a PAN implies the portability of the devices within it. Devices in the PAN are usually small and often battery powered such as laptop computers, personal data assistants
 20 (PDAs), or other wireless devices. There are also protocols for

implementing wireless network access for printers, scanners and other computer peripherals in the personal area network. With such portability, wireless access devices are easily transported between physical areas in the workplace as well as away from the workplace altogether.

Security and safety of data in a network can be jeopardized by uncontrolled access to a network by unauthorized users of wireless access devices, by authorized users in areas exposed to observation by unauthorized persons or computers, by users authorized in some areas but not in others, and by authorized network users with unauthorized devices. Wireless access removes what limited restrictions on access as are provided by wired connection.

Existing means of controlling access to wireless networks are similar to those used in the wired arena. They are typically centralized controls residing in a server in a network and dependent on the physical location of the connection point of the various access devices. Wireless access devices reduce the significance of physical location of connection points and thereby their utility in limiting access to authorized users.

What is needed, then, is means of controlling access to wireless networks, such as personal area networks, in order to provide security for those personal area networks against access by unauthorized users and unauthorized devices. Furthermore, such

5 means should not be dependent on the permanent physical location of a connection point.

CONFIDENTIAL

SUMMARY OF THE INVENTION

Presented herein is a method for controlling access to wireless networks, such as personal area networks, in order to provide security for those personal area networks against access by unauthorized users and unauthorized devices. Furthermore, the method of providing such security is not dependent on the permanent physical location of a connection point.

The present invention relates to a method for managing access to a wireless personal area network in an intelligent concentrator.

10 The method manages wireless access to a network by providing wireless communication in the network, providing firewall protection between the network and a wireless access device, receiving an identification code from the wireless access device to the network, determining whether the identification code is valid, granting network access to the wireless access device when the identification code is valid, denying network access to the wireless access device when the identification code is not valid, and issuing an alert to a network manager when the identification code is not valid. The identification code can be the unique media access code of the wireless access device or any other unique identification code previously registered with the network manager.

These and other objects and advantages of the present invention will become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiments which are illustrated in the various drawing figures.

CONFIDENTIAL

BRIEF DESCRIPTION OF THE DRAWINGS

The operation of this invention can be best visualized by reference to the drawings.

Figure 1 illustrates a local area network with personal area
5 network adjuncts and internet access.

Figure 2 illustrates a physical implementation of one embodiment of the present invention.

Figure 3 illustrates a physical implementation of one embodiment of the present invention.

10 Figure 4 illustrates a physical implementation of one embodiment of the present invention.

Figure 5 illustrates a block flow diagram of one embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Reference will now be made in detail to the preferred
embodiments of the invention, examples of which are illustrated in
the accompanying drawings. While the invention will be described in
5 conjunction with the preferred embodiments, it will be understood
that they are not intended to limit the invention to these
embodiments. On the contrary, the invention is intended to cover
alternatives, modifications and equivalents, which may be included
within the spirit and scope of the invention as defined by the
10 appended claims. Furthermore, in the following detailed description
of the present invention, numerous specific details are set forth in
order to provide a thorough understanding of the present invention.
However, it will be obvious to one of ordinary skill in the art that
the present invention may be practiced without these specific
15 details. In other instances, well-known methods, procedures,
components, and circuits have not been described in detail so as not
to unnecessarily obscure aspects of the present invention.

Some portions of the detailed descriptions that follow are
presented in terms of procedures, logic blocks, processing, and other
20 symbolic representations of operations on signals within an
electronic circuit. These descriptions and representations are the

means used by those skilled in the electronic arts to most effectively convey the substance of their work to others skilled in the art. A procedure, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in an electronic system.

Figure 1 illustrates a local area network that includes server 104 and distributed Intelligent concentrators 100 connected by data lines 120. Intelligent concentrators 100 act as wireless hubs for work centers 110 and 111 which results in each work center being implemented as a Personal Area Network (PAN). Note here that the term "personal area network" typically refers to a small network linked wirelessly to a larger local area network. Work center 112 is a hard-wired work center but acts in every way the same as a personal area networks except for the restricted motion of the hard-wired devices in the work center all connected to an intelligent concentrator 100. Note that the intelligent concentrator referred to in this discussion is one physical implementation of this

embodiment of the present invention. Other embodiments may be implemented in other physical devices.

Personal area network 110 is a typical PAN. It includes wireless access devices 105, a PDA enabled for wireless network access, laptop computer 101, work station 107, and network printer 108. Each of these wireless access devices communicates with intelligent concentrator 100 by means of wireless communication 130 which may be a radio frequency (RF) protocol, such as Bluetooth or some other RF protocol, or infrared (IR).

Note that wireless communication enables and implies a temporary nature to the specific suite of wireless access devices within the personal area network. A user may carry a PDA at all times while moving about the workplace, or even when outside of the workplace, and access the network with it only occasionally.

Data-enabled cell phone 106, shown communicating with intelligent concentrator 135 in personal area network 111, is another highly portable wireless access device that would likely access the wireless network on an occasional basis. Yet another possible wireless access device is illustrated by scanner 109. In this embodiment of the present invention, the intelligent concentrators, 100, are enabled to determine, by this embodiment of the present

invention and upon each attempt to access the network, whether each wireless access device is an authorized device.

An intelligent concentrator, illustrated at 100 in Figure 1, is easy to install and reliably provides a hub and connection point for access to Voice & Data Networks. The embodiment of the present invention discussed here is implemented through miniaturized hardware that could be installed inside a wall or in an internal space provided for in an office cubicle. Power is easily supplied using the same hardware, either locally or remotely over network cabling.

Access to device power is simultaneously accessible with data line connection in a wired connection. Wireless access devices are commonly battery powered or receive power from some other source.

Figure 2 illustrates a possible configuration for the physical implementation of an embodiment of the present invention.

Intelligent concentrator 200 is shown in side cutaway view, with connector jacks 204 for possible wired connections and wireless communication device 207 shown in one of several conceivable arrangements. Wireless communication device 207 is envisioned as being enabled in a variety of protocols. Multiplexing of signals to and from server 104 would very likely be under the control of in-unit electronics suite 202. Those signals, in one embodiment of the

present invention, would be multiplexed onto single cable 100 and connect to intelligent concentrator 200 via back-of-unit connector 206.

Also shown in Figure 2 is an add-on device 203. A range of possibilities exists for the functions of device 203. It could be implemented as an intelligent device, capable of being remotely tested, allowing the network infrastructure and integrity of the network cabling to be tested and evaluated from a central location, without any action being required at the work site. Device 203 can also be implemented as a physical security device, capable of preventing physical attachment to the LAN cabling without a notification being sent to the server that the physical network port has been compromised. Device 203 can also simply be a dust cover installed on an intelligent concentrator that is only involved in a wireless personal area network, obviating the need for wired connectors 204. In one embodiment, wired connectors 204 are implemented as standard communications jacks, such as RJ45. Additionally, status indicator lights are mounted on the surface of the intelligent concentrator in another embodiment.

Figure 3 illustrates one configuration for the user-accessible face of an intelligent concentrator, one physical implementation of

this embodiment of the present invention. Intelligent concentrator 100 is shown here with four RJ-45 jacks, 204. There is space, even if an intelligent concentrator takes the form factor of a standard wall plate device, for more jacks, 308. These other jacks could

5 enable a parallel connection to a different network or to a telephone system independent of a LAN or to a number of other envisioned possibilities. Figure 3 also shows status indicator light 305 which could be implemented in another implementation of this embodiment.

Again shown, in Figure 3, is wireless communication device

10 207. Device 207 can be implemented in any number of wireless standards for wireless connection to the network. The necessary transceiver electronics for device 207 are contained in the body of concentrator 100, integral with internal electronics 202 in Figure 2. Other implementations could implement the circuitry in other ways,

15 however. Power for communications device 207 and its associated circuitry can, like that for intelligent electronic circuitry 202 and device 203, be received via multiplexed cabling.

Figure 4 illustrates one implementation for supplying device power. Here utility socket 320 is shown in order to illustrate the

20 application of high voltage or current power that reaches the intelligent concentrator via cabling parallel to the data cabling.

With access to the power being through intelligent concentrator 200, management and control of a power supply to a device can still be maintained even though the data is communicated wirelessly. The illustration of a utility power socket is not meant to imply that

5 there is some special application of utility AC power in this embodiment. It is solely meant to illustrate a parallel application of high-voltage power through an intelligent concentrator.

Figure 5 illustrates a block flow diagram of one embodiment of the present invention. There, in process 500, a distributed firewall

10 is provided at 510 for each applicable network work center. Network wireless access devices, such as computers, PDAs, data-enabled cell phones, and computer peripherals, attempt network access by submitting a unique identification code which is received by the distributed firewall at 520. At 530, the submitted

15 identification code is compared to a list of valid, registered identification codes. If the submitted code is valid, 540, network access is granted at 570 and the process ends at 599. If the identification code is not valid, network access is denied at 550 and an alert flag is raised to the network manager, 560. Again, the

20 process ends at 599.

A significant advantage offered by this embodiment is in the uniqueness of the list of valid identification codes, in this

embodiment media access codes (MACs), that is supplied to each distributed firewall when the network is started. Note that the MAC (Media Access Control) address is a device's unique hardware number. On an Ethernet LAN, it is generally the same as the device's ethernet address. When a device is connected to the Internet from a computer or host, a correspondence table relates the IP address to the computer's physical address on the LAN.

Each distributed firewall has its own unique identification with the network manager and is given the list of codes applicable to that particular distributed firewall. The network manager, for example, can have a wireless laptop computer whose identification code is on every list issued in the network. Then the network manager can access the network from any personal area network location in the entire network. A personal area network user can have a PDA that is valid for access at the user's workstation and also at a laboratory that the user often works in.

In another example of the utility of this embodiment of the present invention, if two users have personal area networks adjacent to each other, their wireless access devices have unique codes that are not found on each other's applicable valid code list. In that way, restrictions can be implemented that prevent cross-

talk between personal area networks and can also provide a layer of network authorization management.

Some distributed firewalls can be implemented with unlimited valid codes but with limited network access to wireless devices that access the network through those firewalls. This is useful in a company lobby where visitors can use their own wireless access devices to access the network as far as phone directories and promotional information but not as far as entry into restricted network areas.

In one embodiment of the present invention, the distributed firewall is implemented as firmware in an intelligent concentrator. In another embodiment, the firewall is implemented as software in a wireless network hub where it is in control of access from several personal area networks that are centered on the same physical hub. A common thread between these implementations is the distributed access control afforded to the distributed firewalls by the separate maintenance of the valid access code lists.

Each list in this embodiment of the present invention contains information such as a unique firewall identification code, the physical residency and location of the firewall, a list of designated users, and a list of registered MAC addresses. The list of users for a

work station personal area network can be as small as to include only the network manager and the personal area networks primary user. The list for a firewall associated with a conference room, for example, can have no restrictions on users but significant
5 limitations on network resources that are accessible from the conference room.

The number of possible variations in access lists is limited only by network and workplace needs. This embodiment affords an extremely adaptable wireless network access management tool to
10 the network manager.

The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many
15 modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various
20 modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.